Linux KVM での展開（3.2.2 より前のリリース）

Linux KVM で Nexus Dashboard クラスタを展開するための前提条件と注意事項

Linux KVM で Nexus Dashboard クラスタの展開に進む前に、KVM が次の前提条件を満たしている必要があり、次の注意事項に従う必要があります。

- KVM フォーム ファクタが拡張性とサービス要件をサポートする必要があります。

  クラスタ フォーム ファクタに基づいて、拡張性とサービス サポートおよび共同ホストは異なります。Nexus ダッシュボード キャパシティ プランニング ツールを使用して、仮想フォーム ファクタが展開要件を満たすことを確認できます。

- 前提条件：Nexus Dashboard に記載されている一般的な前提条件を確認して完了します。
- 展開予定のサービスのリリース ノートに説明されている追加の前提条件を確認し、条件を満たすようにしてください。
- Nexus Dashboard VM に使用される CPU ファミリが AVX 命令セットをサポートしている必要があります。
- KVM には十分なシステム リソースが必要です。
  - 16 vCPU
  - 64 GB の RAM
  - 550 GBのディスク

    各ノードには専用のディスク パーティションが必要です。

- ディスクの I/O 遅延は 20 ミリ秒以下である必要があります。

  「Linux KVM ストレージ デバイスの I/O 遅延の確認 （2 ページ）」を参照してください。

- KVM の展開は、Nexus Dashboard ファブリック コントローラでのみサポートされます。
- CentOS 7.9 または Red Hat Enterprise Linux 8.6 または 8.8 に展開する必要があります。
- Kernel および KVM のサポートされるバージョンが必要です。
  - CentOS 7.9 の場合、Kernel バージョン `3.10.0-957.el7.x86_64` および KVM バージョン `libvirt-4.5.0-23.el7_7.1.x86_64`
  - RHEL 8.6 の場合、Kernel バージョン `4.18.0-372.9.1.el8.x86_64` および KVM バージョン `libvert 8.0.0`
  - RHEL 8.8 の場合、Kernel バージョン `4.18.0-477.10.1.el8_8.x86_64` および KVM バージョン `libvirt 8.0.0-19`
- 各 Nexus Dashboard ノードは異なる KVM ハイパーバイザに展開することを推奨します。

Linux KVM ストレージ デバイスの I/O 遅延の確認

Linux KVM に Nexus Dashboard クラスタを展開する場合、KVM のストレージ デバイスの遅延は 20 ミリ秒未満である必要があります。

Linux KVM ストレージ デバイスの I/O 遅延を確認するには、次の手順を実行します。

手順

ステップ 1 テスト ディレクトリを作成します。

たとえば、`test-data`という名前のディレクトリを作成します。

ステップ 2 フレキシブル I/O テスター（FIO）を実行します。

```
# fio --rw=write --ioengine=sync --fdatasync=1 --directory=test-data --size=22m --bs=2300 --name=mytest
```

ステップ 3 コマンドの実行後に、`fsync/fdatasync/sync_file_range` セクションの `99.00th=[<value>]` が 20 ミリ秒未満であることを確認します。

Linux KVM での Nexus ダッシュボードの展開

ここでは、Linux KVM で Cisco Nexus ダッシュボード クラスタを展開する方法について説明します。

始める前に

- Linux KVM で Nexus Dashboard クラスタを展開するための前提条件と注意事項 （1 ページ） に記載されている要件とガイドラインを満たしていることを確認します。

手順

ステップ 1 Cisco Nexus ダッシュボード イメージをダウンロードします。

a) [ソフトウェア ダウンロード（Software Download）] ページを参照します。

https://software.cisco.com/download/home/286327743/type/286328258

b) **[Nexus ダッシュボード ソフトウェア]** をクリックします。

c) 左側のサイドバーから、ダウンロードする Nexus ダッシュボードのバージョンを選択します。

d) Linux KVM の Cisco Nexus ダッシュボードイメージをダウンロードします（`nd-dk9.<version>.qcow2`）。

ステップ 2 ノードをホストする Linux KVM サーバーにイメージをコピーします。

`scp` を使用してイメージをコピーできます。次に例を示します。

```
# scp nd-dk9.<version>.qcow2 root@<kvm-host-ip>:/home/nd-base
```

次の手順は、イメージを `/home/nd-base` ディレクトリにコピーしたことを前提としています。

ステップ 3 最初のノードに必要なディスクイメージを作成します。

ダウンロードしたベース `qcow2` イメージのスナップショットを作成し、そのスナップショットをノードの VM のディスク イメージとして使用します。また、ノードごとに2番目のディスクイメージを作成する必要があります。

a) KVM ホストに `root` ユーザとしてログインします。

b) ノードのスナップショット用のディレクトリを作成します。

次の手順は、`/home/nd-node1` ディレクトリにスナップショットを作成することを前提としています。

```
# mkdir -p /home/nd-node1/
# cd /home/nd-node1
```

c) スナップショットを作成します。

次のコマンドで、`/home/nd-base//nd-dk9.<version>.qcow2` を以前のステップで作成したベースイメージの場所に置換します。

```
# qemu-img create -f qcow2 -b /home/nd-base/nd-dk9.<version>.qcow2
/home/nd-node1/nd-node1-disk1.qcow2
```

（注）
RHEL 8.6 で展開する場合は、宛先スナップショットの形式を定義するための追加のパラメータも指定する必要があります。その場合は、上記のコマンドを次のように更新します。

```
# qemu-img create -f qcow2 -b /home/nd-base/nd-dk9.2.1.1a.qcow2
/home/nd-node1/nd-node1-disk1.qcow2 -F qcow2
```

d) ノードの追加ディスクイメージを作成します。

各ノードには 2 つのディスクが必要です。ベースの Nexus ダッシュボード`qcow2`イメージのスナップショットと、2 番目の 500GB ディスクです。

```
# qemu-img create -f qcow2 /home/nd-node1/nd-node1-disk2.qcow2 500G
```

ステップ 4 前のステップを繰り返して、2 番目と 3 番目のノードのディスク イメージを作成します。

次の手順に進む前に、次の準備が必要です。

- 1 つ目のノードの場合、2 つのディスクイメージがある `/home/nd-node1/` ディレクトリ：
  - `/home/nd-node1/nd-node1-disk1.qcow2` は、ステップ 1でダウンロードしたベース `qcow2` イメージのスナップショットです。
  - `/home/nd-node1/nd-node1-disk2.qcow2`。これは、作成した新しい 500GB のディスクです。
- 2 つ目のノードの場合、2つのディスクイメージがある/ home / nd-node2 /ディレクトリ。
  - `/home/nd-node2/nd-node2-disk1.qcow2` は、ステップ 1 でダウンロードした基本 `qcow2` イメージのスナップショットです。
  - `/home/nd-node2/nd-node2-disk2.qcow2`。これは、作成した新しい 500GB のディスクです。
- 3 つ目のノードの場合、2 つのディスク イメージがある `/home/nd-node3/` ディレクトリ。
  - `/home/nd-node1/nd-node3-disk1.qcow2`。ステップ 1 でダウンロードしたベース `qcow2` イメージのスナップショットです。
  - `/home/nd-node1/nd-node3-disk2.qcow2`。これは、作成した新しい 500GB のディスクです。

ステップ 5 最初のノードの VM を作成します。

（注）
Nexus Dashboard リリース 3.2.2 より前のリリースでは、デスクトップ GUI ベースの手順のみがサポートされています。

a) KVM コンソールを開き、**[新しい仮想マシン（New Virtual Machine）]** をクリックします。

コマンド ラインから `virt-manager` コマンドを使用して KVM コンソールを開くことができます。

b) **[新しい VM（New VM）]** 画面で、**[既存のディスク イメージのインポート（import existing disk image）]** オプションを選択し、**[転送（Forward）]** をクリックします。

c) **[既存のストレージ パスを指定（Provide existing storage path）]**フィールドで **[参照（Browse）]** をクリックし、`nd-node1-disk1.qcow2` ファイルを選択します。

各ノードのディスクイメージは、それぞれのディスクパーティションに保存することを推奨します。

d) **OS タイプ**と**バージョン**に対して `[Generic]` を選択し、**[転送]** をクリックします。

e) 64GB のメモリと 16 個の CPU を指定し、**[転送（Forward）]** をクリックします。

f) 仮想マシンの**名前**（例：`nd-node1`）を入力し、**[インストール前に構成をカスタマイズする（Customize configuration before install）]**オプションをオンにします。次に、[完了（Finish）] をクリックします。

（注）

ノードに必要なディスクとネットワークカードをカスタマイズできるようにするには、**[インストール前に構成をカスタマイズする]** チェックボックスをオンにする必要があります。

[VMの詳細]ウィンドウが開きます。

[VMの詳細]ウィンドウで、NICのデバイスモデルを変更します。

a) **NIC <mac>** を選択します。
b) **[デバイス モデル]** で、`[e1000]` を選択します。
c) **[ネットワーク ソース（Network Source）]** で、ブリッジデバイスを選択し、「mgmt」ブリッジの名前を指定します。

（注）
ブリッジデバイスの作成はこのガイドの範囲外であり、配布およびオペレーティング システムのバージョンに依存します。詳細については、オペレーティングシステムのマニュアル（Red Hat の「*Configuring a network bridge*」など）を参照してください。

VMの詳細ウィンドウで、2番目のNICを追加します。

a) [ハードウェアを追加（Add Hardware）] をクリックします。
b) **[新しい仮想ハードウェアの追加（Add new virtual hardware）]** ウィンドウで、**[ネットワーク]** を選択します。
c) **[ネットワーク ソース（Network Source）]** で、ブリッジデバイスを選択し、作成した「データ」ブリッジの名前を指定します。
d) デフォルトの **MAC アドレス** の値のままにします。
e) **[デバイス モデル]** で、`[e1000]` を選択します。

[VMの詳細（VM details）] ウィンドウで、2 番目のディスク イメージを追加します。

a) [ハードウェアを追加（Add Hardware）] をクリックします。
b) **[新しい仮想ハードウェアの追加]** 画面で、**[ストレージ]** を選択します。
c) ディスクのバス ドライバについては、`[IDE]` を選択します。
d) **[カスタム ストレージの選択または作成（Select or create custom storage）]** を選択し、**[管理（Manage）]** をクリックして、作成した `nd-node1-disk2.qcow2` ファイルを選択します。
e) **[終了（Finish）]** をクリックして 2 番目のディスクを追加します。

（注）
仮想マシン マネージャの UI で `[ホスト CPU 設定のコピー（Copy host CPU configuration）]` オプションが有効になっていることを確認します。

最後に、**[インストールの開始（Begin Installation）]** をクリックして、ノードのVMの作成を終了します。

ステップ 6 以前のステップを繰り返し、2 番目と 3 番目のノードを展開して、すべての VM を開始します。

（注）
単一のノードクラスタを展開している場合は、この手順をスキップできます。

ステップ 7 ノードのコンソールのいずれかを開き、ノードの基本情報を設定します。Linux KVM 環境にデスクトップ GUI がない場合は、 virsh コンソールを 実行します。<node-name>コマンドを使用して、ノードのコンソールにアクセスします。

a) いずれかのキーを押して、初期設定を開始します。

初回セットアップユーティリティの実行を要求するプロンプトが表示されます。

```
[ OK ] Started atomix-boot-setup.
       Starting Initial cloud-init job (pre-networking)...
       Starting logrotate...
       Starting logwatch...
       Starting keyhole...
[ OK ] Started keyhole.
[ OK ] Started logrotate.
[ OK ] Started logwatch.

Press any key to run first-boot setup on this console...
```

b) admin パスワードを入力して確認します。

このパスワードは、rescue-user SSH ログインおよび初期 GUI パスワードに使用されます。

（注）
すべてのノードに同じパスワードを指定する必要があります。指定しない場合、クラスタ作成に失敗します。

```
Admin Password:
Reenter Admin Password:
```

c) 管理ネットワーク情報を入力します。

```
Management Network:
  IP Address/Mask: 192.168.9.172/24
  Gateway: 192.168.9.1
```

d) 最初のノードのみ、「クラスタ リーダー」として指定します。

クラスタ リーダー ノードにログインして、設定を完了し、クラスタの作成を完了します。

```
Is this the cluster leader?: y
```

e) 入力した譲歩をレビューし、確認します。

入力した情報を変更するかどうかを尋ねられます。すべてのフィールドが正しい場合は、n を選択して続行します。入力した情報を変更する場合は、y を入力して基本設定スクリプトを再起動します。

```
Please review the config
Management network:
  Gateway: 192.168.9.1
  IP Address/Mask: 192.168.9.172/24
Cluster leader: yes

Re-enter config? (y/N): n
```

ステップ 8 前の手順を繰り返して、2 番目と 3 番目のノードの初期情報を構成します。

最初のノードの設定が完了するのを待つ必要はありません。他の 2 つのノードの設定を同時に開始できます。

（注）

すべてのノードに同じパスワードを指定する必要があります。指定しない場合、クラスタ作成に失敗します。

2 番目と 3 番目のノードを展開する手順は同じですが、**クラスタ リーダー**ではないことを示す必要がある点が異なります。

ステップ 9 初期ブートストラップ プロセスを待機して、すべてのノードで完了します。

管理ネットワーク情報を入力して確認すると、最初のノード（クラスタ リーダー）初期設定でネットワーキングが設定され、UI が表示されます。この UI を使用して、他の 2 つのノードを追加し、クラスタの展開を完了します。

```
Please wait for system to boot: [#########################] 100%
System up, please wait for UI to be online.

System UI online, please login to https://192.168.9.172 to continue.
```

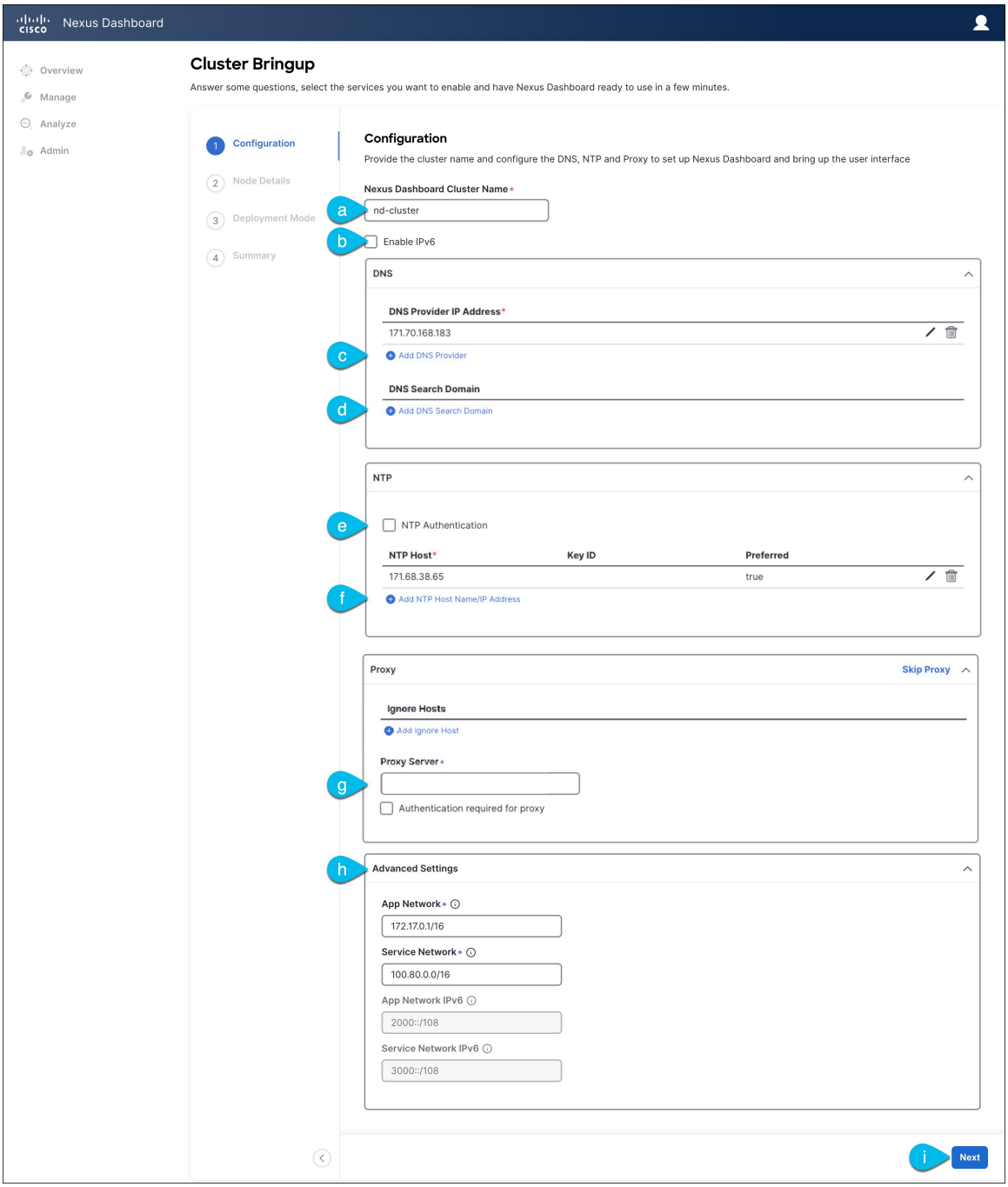
ステップ 10 ブラウザを開き、`https://<node-mgmt-ip>` に移動して、GUI を開きます。

残りの設定ワークフローは、ノードの GUI の 1 つから実行します。展開したノードのいずれか 1 つを選択して、ブートストラッププロセスを開始できます。他の 2 つのノードにログインしたり、これらを直接構成したりする必要はありません。

前の手順で入力したパスワードを入力し、**[ログイン（Login）]** をクリックします。

ステップ 11 **[クラスタの詳細（Cluster Details）]** を入力します。

[クラスタ起動（Cluster Bringup）] ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。



a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** を入力します。

- クラスタ名は、 RFC-1123 の要件に従う必要があります。
- マルチクラスター接続を使用して複数の Nexus Dashboard クラスター間の接続を確立する場合は、一緒に接続する予定のクラスターの名前が一意である必要があります。

b) （オプション）クラスタの IPv6 機能を有効にする場合は、**[IPv6 を有効にする（Enable IPv6）]** チェックボックスをオンにします。

c) **[+DNS プロバイダの追加（+Add DNS Provider）]** をクリックして、1 つ以上の DNS サーバを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

d) （オプション）**[+DNS 検索ドメインの追加（+Add DNS Search Domain ）]** をクリックして、検索ドメインを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

e) （オプション）NTP サーバー認証を有効にする場合には、**[NTP 認証（NTP Authentication）]** チェックボックスをオンにし、**[NTP キーの追加（Add NTP Key）]** をクリックします。

次のフィールドで、以下の情報を提供します。

- **NTP キー**：Nexus ダッシュボードと NTP サーバ間の NTP トラフィックを認証するために使用される暗号キー。次の手順で NTP サーバーを定義します。複数の NTP サーバで同じ NTP キーを使用できます。
- **キー ID**：各 NTP キーに一意のキー ID を割り当てる必要があります。この ID は、NTP パケットの検証時に使用する適切なキーを識別するために使用されます。
- **認証タイプ**：このリリースでは、`MD5`、`SHA`、および `AES128CMAC` 認証タイプがサポートされています。
- このキーが**信頼**できるかどうかを選択します。信頼できないキーは NTP 認証に使用できません。

（注）
情報を入力した後、チェックマーク アイコンをクリックして保存します。

NTP 認証の要件とガイドラインの完全なリストについては、すべての有効なサービスの前提条件と注意事項 を参照してください。

f) **[+ NTP ホスト名/IP アドレスの追加（+Add NTP Host Name/IP Address）]** をクリックして、1 つ以上の NTP サーバを追加します。

次のフィールドで、以下の情報を提供します。

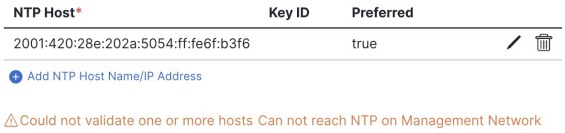
- **NTP ホスト**：IP アドレスを指定する必要があります。完全修飾ドメイン名（FQDN）はサポートされていません。
- **キー ID**：このサーバーの NTP 認証を有効にする場合は、前の手順で定義した NTP キーのキー ID を指定します。

  NTP 認証が無効になっている場合、このフィールドはグレー表示されます。
- この NTP サーバーを **[優先（Preferred）]** にするかどうかを選択します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

（注）

ログインしているノードに IPv4 アドレスのみが設定されているが、前の手順で [IPv6 を有効にする（Enable IPv6）] をオンにして NTP サーバーの IPv6 アドレスを指定した場合は、次の検証エラーが表示されます。



これは、ノードに IPv6 アドレスがまだなく（次の手順で指定します）、NTP サーバーの IPv6 アドレスに接続できないためです。

この場合、次の手順の説明に従って他の必要な情報の入力を完了し、**[次へ（Next）]** をクリックして次の画面に進み、ノードの IPv6 アドレスを入力します。

追加の NTP サーバーを指定する場合は、**[+NTP ホストの追加（+Add NTP Host）]** を再度クリックし、このサブステップを繰り返します。

g) **[プロキシ サーバー（Proxy Server）]** を指定し、**[検証（Validate）]** をクリックします。

Cisco Cloud に直接接続できないクラスタの場合は、接続を確立するためにプロキシ サーバを構成することをお勧めします。これにより、ファブリック内の非適合ハードウェアおよびソフトウェアにさらされるリスクを軽減できます。

[+無視するホストを追加（+Add Ignore Host）] をクリックして、プロキシをスキップする 1 つ以上の IP アドレス通信を提供することもできます。

プロキシ サーバーでは、次の URL が有効になっている必要があります。

```
dcappcenter.cisco.com
svc.intersight.com
svc.ucs-connect.com
svc-static1.intersight.com
svc-static1.ucs-connect.com
```

プロキシ設定をスキップする場合は、**[プロキシをスキップ（Skip Proxy）]** をクリックします。

h) (オプション) プロキシ サーバで認証が必要な場合は、**[プロキシで認証が必要（Authentication required for Proxy）]** を **[はい（Yes）]** に変更し、ログイン資格情報を指定します。

i) (オプション) **[詳細設定（Advanced Settings）]** カテゴリを展開し、必要に応じて設定を変更します。

詳細設定では、次の設定を行うことができます。

- カスタム **App Network** と **Service Network** を提供します。

  アプリケーション オーバーレイ ネットワークは、Nexus ダッシュボードで実行されるアプリケーションのサービスで使用されるアドレス空間を定義します。このフィールドには、デフォルトの `172.17.0.1/16` 値が事前に入力されています。

  サービス ネットワークは、Nexus ダッシュボードとそのプロセスで使用される内部ネットワークです。このフィールドには、デフォルトの `100.80.0.0/16` 値が事前に入力されています。

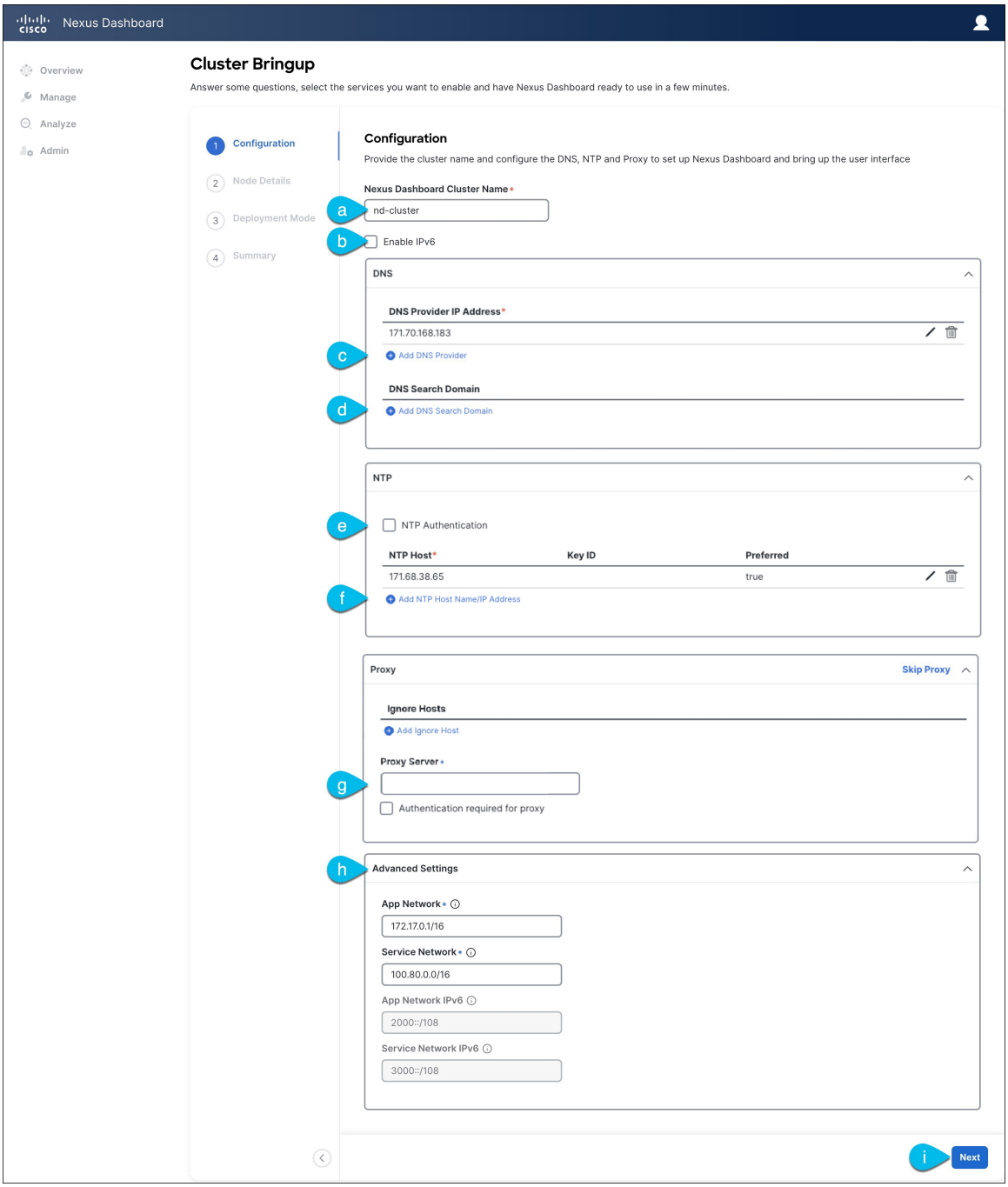
以前に **[IPv6 を有効にする（Enable IPv6）]** オプションをオンにした場合は、アプリケーション ネットワークとサービス ネットワークの IPv6 サブネットを定義することもできます。

アプリケーションおよびサービスネットワークについては、このドキュメントの前の すべての有効なサービスの前提条件と注意事項 の項で説明します。

j) **[次へ（Next）]** をクリックして続行します。

ステップ 12 **[クラスタの詳細（Cluster Details）]** を入力します。

[クラスタ起動（Cluster Bringup）] ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。



a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** を入力します。

- クラスタ名は、 RFC-1123 の要件に従う必要があります。
- マルチクラスター接続を使用して複数の Nexus Dashboard クラスター間の接続を確立する場合は、一緒に接続する予定のクラスターの名前が一意である必要があります。

b) （オプション）クラスタの IPv6 機能を有効にする場合は、**[IPv6 を有効にする（Enable IPv6）]** チェックボックスをオンにします。

c) **[+DNS プロバイダの追加（+Add DNS Provider）]** をクリックして、1 つ以上の DNS サーバを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

d) （オプション）**[+DNS 検索ドメインの追加（+Add DNS Search Domain ）]** をクリックして、検索ドメインを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

e) （オプション）NTP サーバー認証を有効にする場合には、**[NTP 認証（NTP Authentication）]** チェックボックスをオンにし、**[NTP キーの追加（Add NTP Key）]** をクリックします。

次のフィールドで、以下の情報を提供します。

- **NTP キー**：Nexus ダッシュボードと NTP サーバ間の NTP トラフィックを認証するために使用される暗号キー。次の手順で NTP サーバーを定義します。複数の NTP サーバで同じ NTP キーを使用できます。
- **キー ID**：各 NTP キーに一意のキー ID を割り当てる必要があります。この ID は、NTP パケットの検証時に使用する適切なキーを識別するために使用されます。
- **認証タイプ**：このリリースでは、`MD5`、`SHA`、および `AES128CMAC` 認証タイプがサポートされています。
- このキーが**信頼**できるかどうかを選択します。信頼できないキーは NTP 認証に使用できません。

（注）
情報を入力した後、チェックマーク アイコンをクリックして保存します。

NTP 認証の要件とガイドラインの完全なリストについては、すべての有効なサービスの前提条件と注意事項 を参照してください。

f) **[+ NTP ホスト名/IP アドレスの追加（+Add NTP Host Name/IP Address）]** をクリックして、1 つ以上の NTP サーバを追加します。

次のフィールドで、以下の情報を提供します。

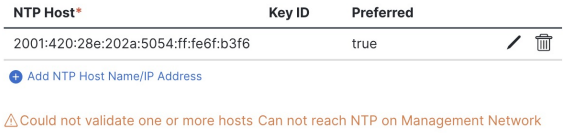
- **NTP ホスト**：IP アドレスを指定する必要があります。完全修飾ドメイン名（FQDN）はサポートされていません。
- **キー ID**：このサーバーの NTP 認証を有効にする場合は、前の手順で定義した NTP キーのキー ID を指定します。

  NTP 認証が無効になっている場合、このフィールドはグレー表示されます。
- この NTP サーバーを **[優先（Preferred）]** にするかどうかを選択します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

（注）

ログインしているノードに IPv4 アドレスのみが設定されているが、前の手順で [IPv6 を有効にする（Enable IPv6）] をオンにして NTP サーバーの IPv6 アドレスを指定した場合は、次の検証エラーが表示されます。



これは、ノードに IPv6 アドレスがまだなく（次の手順で指定します）、NTP サーバーの IPv6 アドレスに接続できないためです。

この場合、次の手順の説明に従って他の必要な情報の入力を完了し、**[次へ（Next）]** をクリックして次の画面に進み、ノードの IPv6 アドレスを入力します。

追加の NTP サーバーを指定する場合は、**[+NTP ホストの追加（+Add NTP Host）]** を再度クリックし、このサブステップを繰り返します。

g) **[プロキシ サーバー（Proxy Server）]** を指定し、**[検証（Validate）]** をクリックします。

Cisco Cloud に直接接続できないクラスタの場合は、接続を確立するためにプロキシ サーバを構成することをお勧めします。これにより、ファブリック内の非適合ハードウェアおよびソフトウェアにさらされるリスクを軽減できます。

[+無視するホストを追加（+Add Ignore Host）] をクリックして、プロキシをスキップする 1 つ以上の IP アドレス通信を提供することもできます。

プロキシ サーバーでは、次の URL が有効になっている必要があります。

```
dcappcenter.cisco.com
svc.intersight.com
svc.ucs-connect.com
svc-static1.intersight.com
svc-static1.ucs-connect.com
```

プロキシ設定をスキップする場合は、**[プロキシをスキップ（Skip Proxy）]** をクリックします。

h) (オプション) プロキシ サーバで認証が必要な場合は、**[プロキシで認証が必要（Authentication required for Proxy）]** を **[はい（Yes）]** に変更し、ログイン資格情報を指定します。

i) (オプション) **[詳細設定（Advanced Settings）]** カテゴリを展開し、必要に応じて設定を変更します。

詳細設定では、次の設定を行うことができます。

- カスタム **App Network** と **Service Network** を提供します。

  アプリケーション オーバーレイ ネットワークは、Nexus ダッシュボードで実行されるアプリケーションのサービスで使用されるアドレス空間を定義します。このフィールドには、デフォルトの `172.17.0.1/16` 値が事前に入力されています。

  サービス ネットワークは、Nexus ダッシュボードとそのプロセスで使用される内部ネットワークです。このフィールドには、デフォルトの `100.80.0.0/16` 値が事前に入力されています。

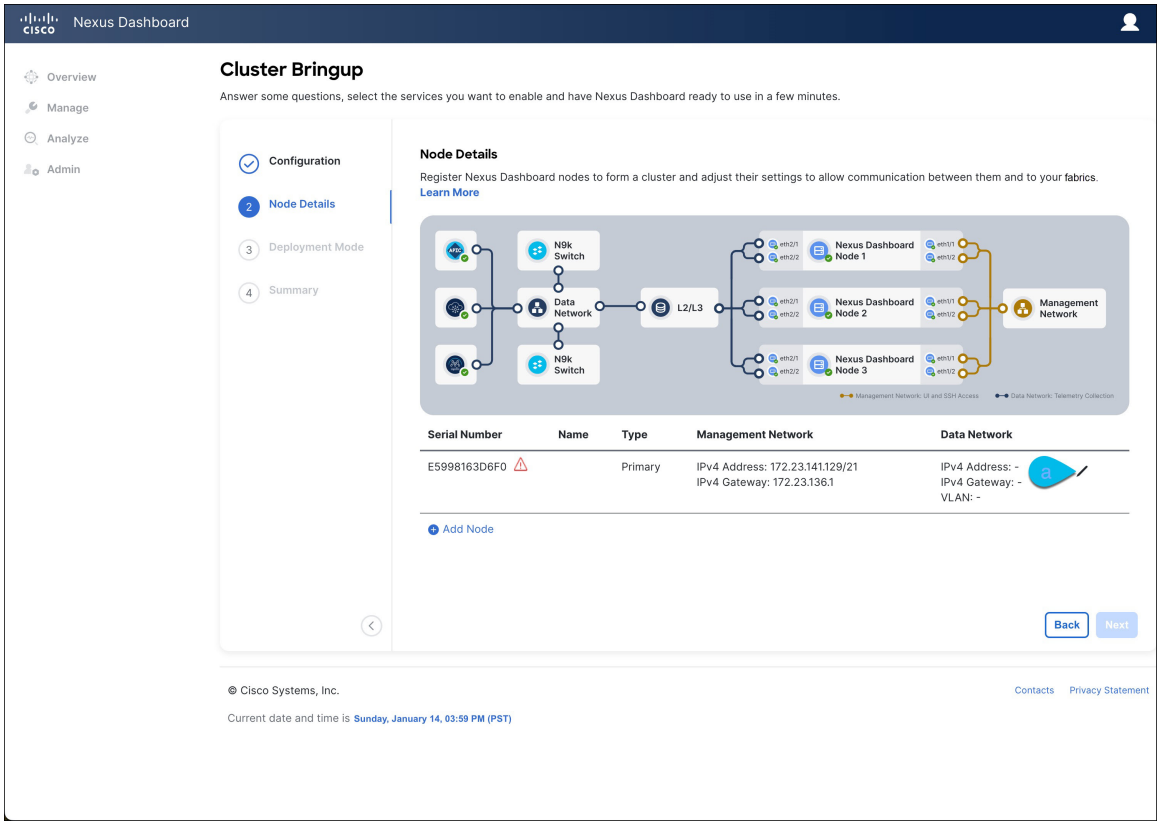
以前に **[IPv6 を有効にする（Enable IPv6）]** オプションをオンにした場合は、アプリケーション ネットワークとサービス ネットワークの IPv6 サブネットを定義することもできます。

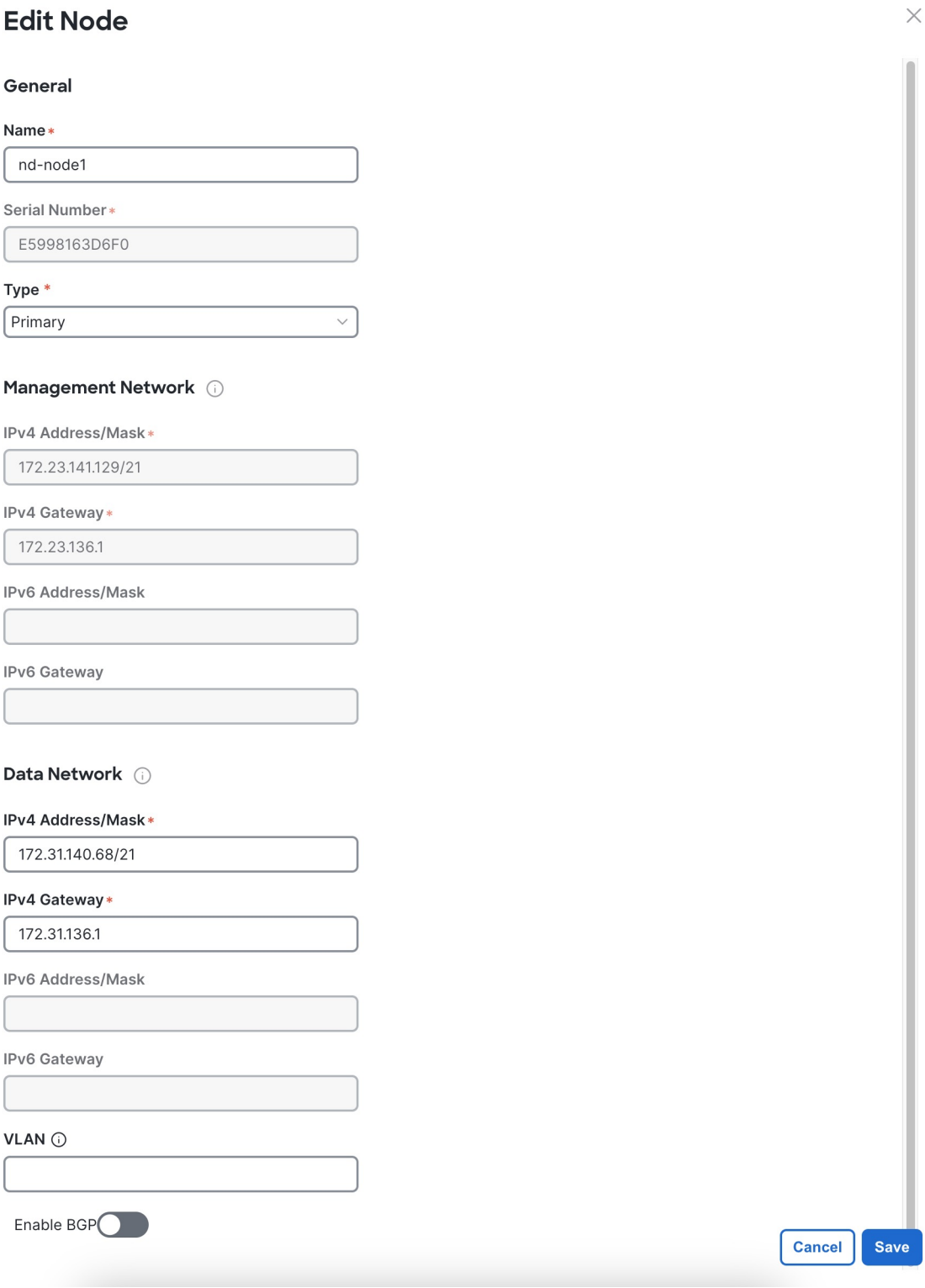
アプリケーションおよびサービスネットワークについては、このドキュメントの前の すべての有効なサービスの前提条件と注意事項 の項で説明します。

j) **[次へ（Next）]** をクリックして続行します。

ステップ 13 **[ノードの詳細（Node Details）]** 画面で、最初のノードの情報を更新します。

前の手順の初期ノード構成時に現在ログインしているノードの管理ネットワークと IP アドレスを定義しましたが、他のプライマリ ノードを追加し、クラスタを作成する進む前に、ノードのデータ ネットワーク情報も指定する必要があります。





a) 最初のノードの横にある **[編集（Edit）]**ボタンをクリックします。

ノードの**[シリアル番号（Serial Number）]**、**[管理ネットワーク（Management Network）]**情報、および**[タイプ（Type）]**が自動的に入力されます。ただし、他の情報は手動で入力する必要があります。

b) ノードの **[名前（Name）]** を入力します。

ノードの **名前** はホスト名として設定されるため、 RFC-1123 の要件に従う必要があります。

c) **[タイプ（Type）]** ドロップダウンから `[プライマリ（Primary）]` を選択します。

クラスタの最初の 3 つのノードは `[プライマリ（ Primary）]` に設定する必要があります。サービスの共同ホスティングや、より大規模なスケールを有効にする必要がある場合は、後の手順でセカンダリ ノードを追加します。

d) **[データ ネットワーク（Data Network）]** エリアで、ノードの**データ ネットワーク**を提供します。

データ ネットワークの IP アドレス、ネットマスク、およびゲートウェイを指定する必要があります。オプションで、ネットワークの VLAN ID を指定することもできます。ほとんどの導入では、[VLAN ID] フィールドを空白のままにできます。

前の画面で IPv6 機能を有効にした場合は、IPv6 アドレス、ネットマスク、およびゲートウェイも入力する必要があります。

（注）
IPv6 情報を提供する場合は、クラスタ ブートストラップ プロセス中に行う必要があります。後で IP 構成を変更するには、クラスタを再展開する必要があります。

クラスタ内のすべてのノードは、 IPv4 のみ、IPv6 のみ、またはデュアル スタック IPv4/IPv6 のいずれかで構成する必要があります。

e) （オプション）クラスタが L3 HA モードで展開されている場合は、データ ネットワークの **[BGP を有効にする（Enable BGP）]** をオンにします。

Insights やファブリック コントローラなどの、一部のサービスで使用される永続的な IP 機能には、BGP 構成が必要です。この機能については、すべての有効なサービスの前提条件と注意事項と『*Cisco Nexus Dashboard* ユーザーガイド』の「永続的な IP アドレス」セクションで詳しく説明されています。

（注）
BGP をこの時点で、またはクラスタの展開後に Nexus ダッシュボード GUI で有効にすることができます。BGP が構成されている場合は、残りのすべてのノードで BGP を構成する必要があります。

BGP を有効にする際、次の情報も入力する必要があります。

- このノードの **ASN**（BGP 自律システム番号）。

  すべてのノードに同じ ASN を構成することも、ノードごとに異なる ASN を構成することもできます。

- 純粋な IPv6 の場合、このノードの**ルータ ID**。

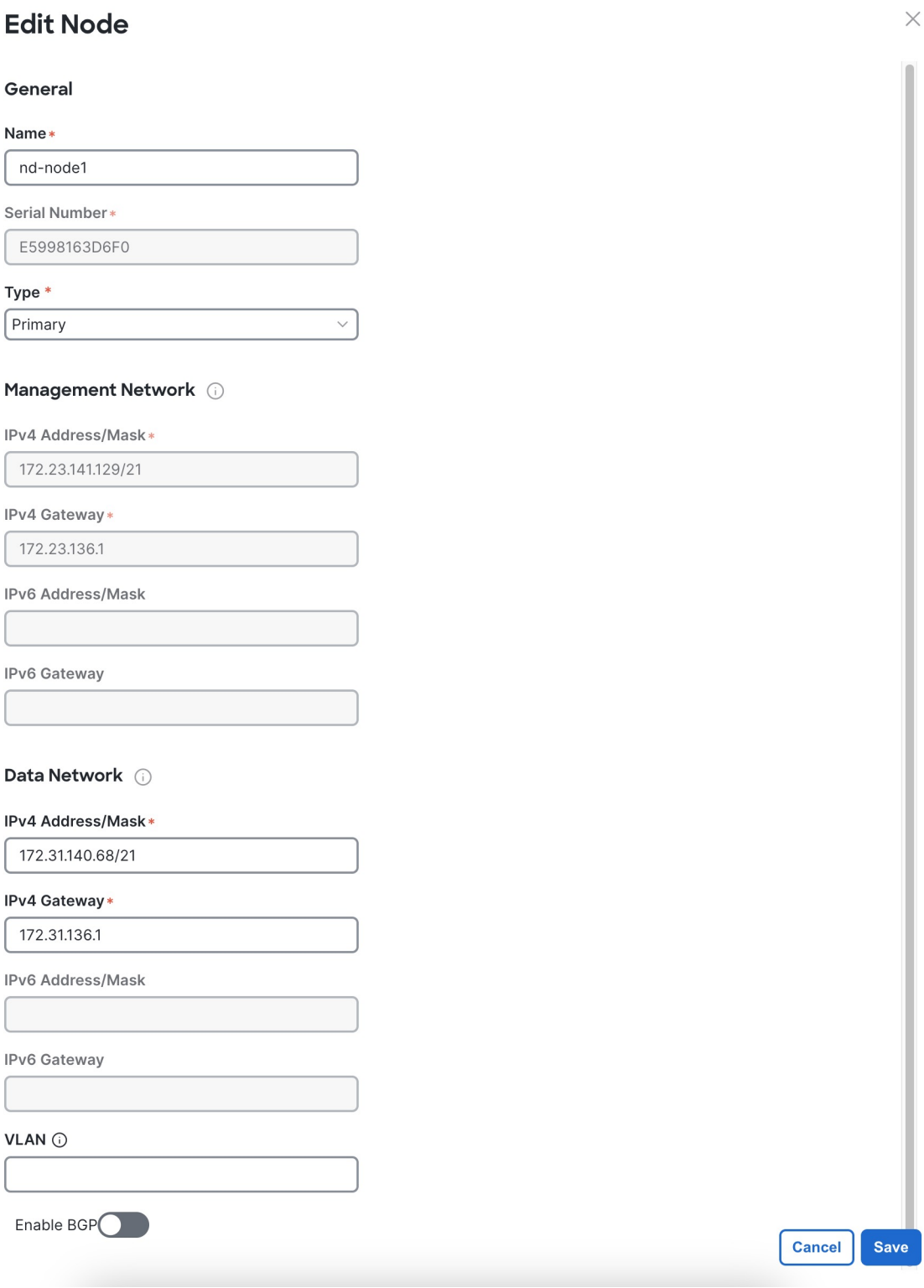
  ルータ ID は、`1.1.1.1` などの IPv4 アドレスである必要があります。

- ピアの IPv4 または IPv6 アドレスとピアの ASN を含む **BGP ピアの詳細**。

f) **[Save]**をクリックして、変更内容を保存します。

ステップ 14 [ノードの詳細（**Node Details**）] 画面で、[ノードの追加（**Add Node**）] をクリックして、クラスタに 2 番目のノードを追加します。

単一ノード クラスタを展開する場合は、この手順をスキップします。



a) **[展開の詳細（Deployment Details）]** エリアで、2 番目のノードに **[管理 IP アドレス（Management IP Address）]** および **[パスワード（Password）]** を指定します。

ノードの初期構成手順で、管理ネットワーク情報とパスワードを定義しました。

b) **[検証（Validate）]** をクリックして、ノードへの接続を確認します。

接続が検証されると、ノードの**シリアル番号**と**管理ネットワーク**情報が自動的に入力されます。

c) ノードの **[名前（Name）]** を入力します。

d) **[タイプ（Type）]** ドロップダウンから `[プライマリ（Primary）]` を選択します。

クラスタの最初の 3 つのノードは `[プライマリ（ Primary）]` に設定する必要があります。サービスの共同ホスティングや、より大規模なスケールを有効にする必要がある場合は、後の手順でセカンダリ ノードを追加します。

e) **[データ ネットワーク（Data Network）]** エリアで、ノードの**データ ネットワーク**を提供します。

データ ネットワークの IP アドレス、ネットマスク、およびゲートウェイを指定する必要があります。オプションで、ネットワークの VLAN ID を指定することもできます。ほとんどの導入では、[VLAN ID] フィールドを空白のままにできます。

前の画面で IPv6 機能を有効にした場合は、IPv6 アドレス、ネットマスク、およびゲートウェイも入力する必要があります。

（注）
IPv6 情報を提供する場合は、クラスタ ブートストラップ プロセス中に行う必要があります。後で IP 構成を変更するには、クラスタを再展開する必要があります。

クラスタ内のすべてのノードは、 IPv4 のみ、IPv6 のみ、またはデュアル スタック IPv4/IPv6 のいずれかで構成する必要があります。

f) （オプション）クラスタが L3 HA モードで展開されている場合は、データ ネットワークの **[BGP を有効にする（Enable BGP）]** をオンにします。

Insights やファブリック コントローラなどの、一部のサービスで使用される永続的な IP 機能には、BGP 構成が必要です。この機能については、すべての有効なサービスの前提条件と注意事項と『*Cisco Nexus Dashboard* ユーザーガイド』の「永続的な IP アドレス」セクションで詳しく説明されています。

（注）
BGP をこの時点で、またはクラスタの展開後に Nexus ダッシュボード GUI で有効にすることができます。

BGP を有効にする際、次の情報も入力する必要があります。

- このノードの **ASN**（BGP 自律システム番号）。

  すべてのノードに同じ ASN を構成することも、ノードごとに異なる ASN を構成することもできます。

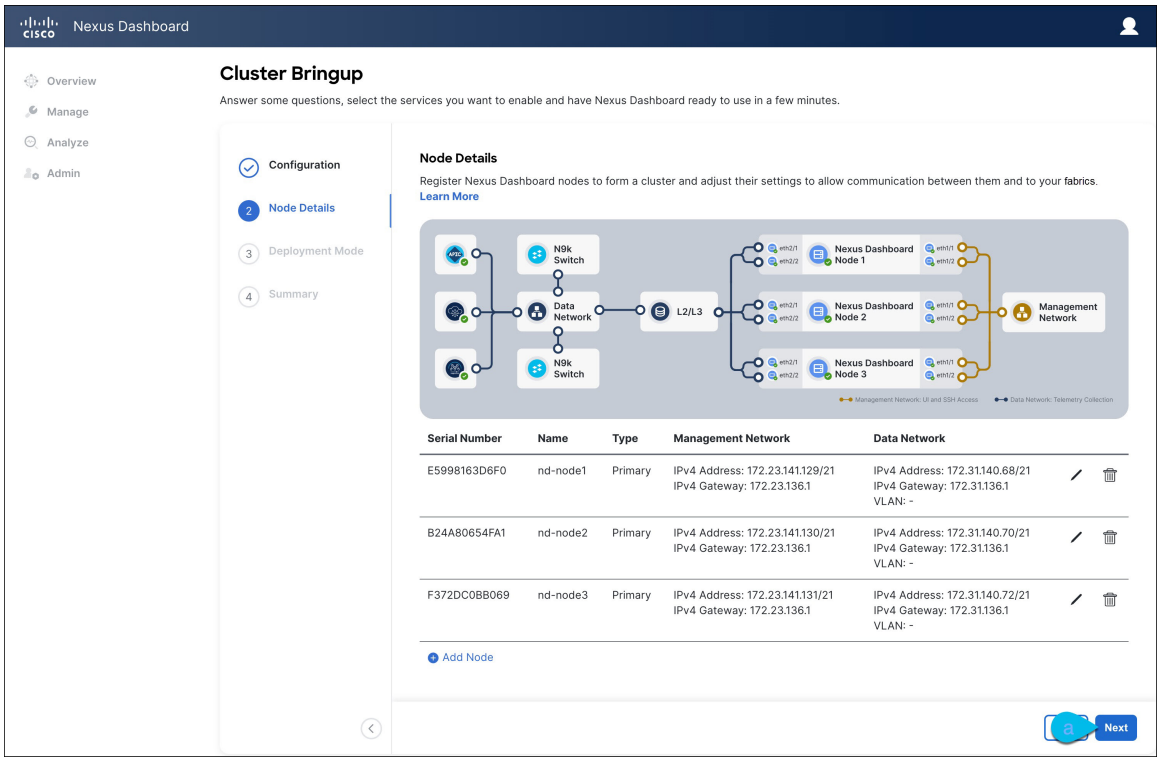
- 純粋な IPv6 の場合、このノードの**ルータ ID**。

  ルータ ID は、`1.1.1.1` などの IPv4 アドレスである必要があります。

- ピアの IPv4 または IPv6 アドレスとピアの ASN を含む **BGP ピアの詳細**。

g) **[Save]**をクリックして、変更内容を保存します。
h) クラスタの最後の（3 番目の）プライマリ ノードでこの手順を繰り返します。

ステップ 15 **[ノードの詳細（Node Details）]** ページで、入力した情報を確認し、**[次へ（Next）]** をクリックして続行します。



ステップ 16 クラスタの**展開モード**を選択します。

a) 有効にするサービスを選択します。

リリース 3.1(1) より前では、クラスタの初期展開が完了した後に、個々のサービスをダウンロードしてインストールする必要がありました。今では、初期インストール時にサービスを有効にするように選択できます。

（注）
クラスタ内のノードの数によっては、一部のサービスまたは共同ホスティングのシナリオがサポートされない場合があります。必要な数のサービスを選択できない場合は、**[戻る（Back）]** をクリックし、前の手順で十分な数のセカンダリ ノードを指定したことを確認します。

b) **[永続サービス IP/プールの追加（Add Persistent Service IPs/Pools）]** をクリックして、Insights またはファブリック コントローラ サービスに必要な 1 つ以上の永続 IP を指定します。

永続的 IP の詳細については、ユーザー ガイドのすべての有効なサービスの前提条件と注意事項のセクションを参照してください。

c) [次へ（Next）] をクリックして続行します。

ステップ 17 **[サマリー（Summary）]** 画面で設定情報を見直して確認し、**[保存（Save）]** をクリックしてクラスタを構築します。

ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

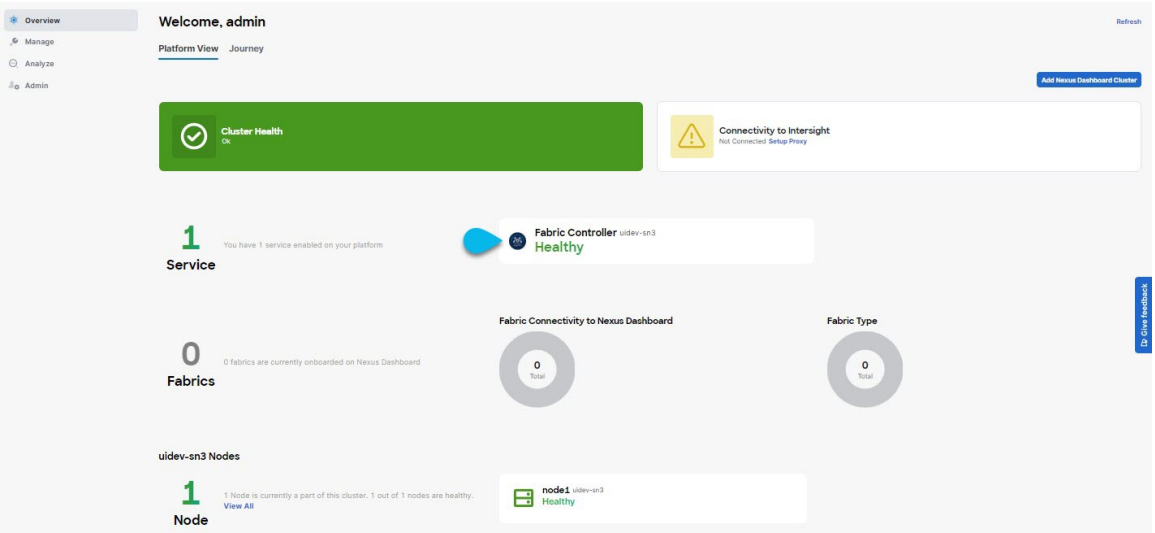
クラスタが形成され、すべてのサービスが開始されるまでに最大30分かかる場合があります。クラスタの設定が完了すると、ページが Nexus ダッシュボード GUI にリロードされます。

ステップ 18 クラスタが健全であることを検証します。

展開モードに応じて、クラスタが形成されすべてのサービスが開始されるまでに最大30分かかる場合があります。

クラスタが使用可能になったら、ノードの管理 IP アドレスのいずれかを参照してアクセスできます。`admin` ユーザーのデフォルト パスワードは、最初のノードに選択した `rescue-user` のパスワードと同じです。この間、UIは上部に「サービスのインストールが進行中です。Nexus Dashboard の設定タスクは現在無効になっています」という意味のバナーを表示します。

すべてのクラスタが展開され、すべてのサービスが開始されたら、**[概要（Overview）]** ページでクラスタが正常であることを確認できます。



または、SSH を使用し、`rescue-user` として、ノード展開中に指定したパスワードを使っていずれかのノードにログインし、`acs health` コマンドを実行してクラスタの状態を確認できます。

- クラスタが収束している間、次の出力が表示されることがあります。

```
$ acs health
k8s install is in-progress
```

```
$ acs health
k8s services not in desired state - [...]
```

```
$ acs health
k8s: Etcd cluster is not ready
```

- クラスタが稼働している場合は、次の出力が表示されます。

```
$ acs health
All components are healthy
```

（注）
場合によっては、ノードの電源を再投入（電源をオフにしてから再度オン）すると、この段階でスタックが停止することがある可能性があります。

```
deploy base system services
```

これは、pND（物理 Nexus Dashboard）クラスタの再起動後のノードの `etcd` の問題が原因です。

この問題を解決するには、影響を受けるノードで `acs reboot clean` コマンドを入力します。

ステップ 19 Nexus Dashboard とサービスを展開したら、設定と操作の記事の説明に従って各サービスを設定できます。

- ファブリック コントローラについては、*NDFC* ペルソナ設定 のホワイトペーパーとドキュメントライブラリを参照してください。
- Orchestrator については、 ドキュメント ページを参照してください。
- Insights については、 ドキュメント ライブラリを参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。